Appendix A: Linguaggio di Scripting delle Transazioni: Operatori, Costanti e Simboli

Mette un valore nello stack mostra gli operatori per immettere valori sullo stack.

Table 1. Mette un valore nello stack

Simbolo	Valore (hex)	Descrizione
OP_0 or OP_FALSE	0x00	Un array vuoto è immesso nello stack
1-75	0x01-0x4b	Metti i prossimi N byte sullo stack dove N è da 1 a 75 byte
OP_PUSHDATA1	0x4c	Il prossimo byte script contiene N, immetti i seguenti N byte nello stack
OP_PUSHDATA2	0x4d	I prossimi due script byte contengono N, metti i seguenti N byte sullo stack
OP_PUSHDATA4	0x4e	I prossimi quattro script byte contengono N, metti i seguenti N byte sullo stack
OP_1NEGATE	0x4f	Metti (push) il valore "–1" sullo stack
OP_RESERVED	0x50	Halt - Transazione non valida a meno che non sia eseguita la clausola OP_IF
OP_1 or OP_TRUE	0x51	Metti il valore "1" sullo stack
OP_2 to OP_16	0x52 to 0x60	Per OP_N, metti il valore "N" sullo stack. Es. OP_2 mette "2"

Flow control condizionale mostra gli operatori di flusso condizionale.

Table 2. Flow control condizionale

Simbolo	Valore (hex)	Descrizione
OP_NOP	0x61	Non eseguire niente
OP_VER	0x62	Interrompi - Transazione Invalida a meno che non sia trovata in una clause OP_IF inaspettata
OP_IF	0x63	Esegui le istruzioni continuando se la cima dello stack non è 0
OP_NOTIF	0x64	Esegui le istruzioni continuando se la cima dello stack è 0

Simbolo	Valore (hex)	Descrizione
OP_VERIF	0x65	Interrompi (Halt) - Transazione non valida
OP_VERNOTIF	0x66	Interrompi (Halt) - Transazione non valida
OP_ELSE	0x67	Esegui solo se le istruzioni precedenti non erano state eseguite
OP_ENDIF	0x68	Finel del blocco OP_IF, OP_NOTIF, OP_ELSE
OP_VERIFY	0x69	Controlla la in cima allo stack, interrompi e invalida la transazione se non TRUE
OP_RETURN	0x6a	Interrompi e invalida la transazione

Stack operations mostra gli operatori usati per manipolare lo stack.

Table 3. Stack operations

Simbolo	Valore (hex)	Descrizione
OP_TOALTSTACK	0x6b	Pop (prendi) dell'elemento dallo stack e mettilo (push) sullo stack alternativo (altstack)
OP_FROMALTSTACK	0x6c	Prendi il primo elemento dell'altstack e mettilo sullo stack
OP_2DROP	0x6d	Prendi i primi due elementi dello stack
OP_2DUP	0x6e	Duplica i due elementi in cima allo stack
OP_2DUP	0x6e	Duplica i tre elementi in cima allo stack
OP_2OVER	0x70	Copia il terzo e il quarto elemento nello stack e metti le copie in cima
OP_2ROT	0x71	Muovi il quinto e il sesto elemento nello stack in cima ad esso
OP_2SWAP	0x72	Scambia le due paia di elementi in cima allo stack
OP_IFDUP	0x73	Duplica l'elemento in cima allo stack se esso non è 0
OP_DEPTH	0x74	Conta gli elementi sullo stack e immetti il valore (del count) risultante sullo stack

Simbolo	Valore (hex)	Descrizione
OP_DROP	0x75	Prendi l'elemento in cima allo stack
OP_DUP	0x76	Duplica l'elemento in cima allo stack
OP_NIP	0x77	Prendi il secondo elemento presente nello stack
OP_OVER	0x78	Copia il secondo elemento nello stack e mettilo in cima
OP_PICK	0x79	Prendi il valore N dalla cima, poi copia l'Nesimo elemento in cima allo stack
OP_ROLL	0x7a	Prendi il valore N dalla cima, poi muovi l'Nesimo elemento in cima allo stack
OP_ROT	0x7b	Ruota i tre elementi in cima allo stack
OP_SWAP	0x7c	Scambia i tre elementi in cima allo stack
OP_TUCK	0x7d	Copia l'elemento situato in cima e inseriscilo tra l'elemento in cima e il secondo elemento.

string Operazioni di concatenamento di stringhe mostra gli operatori applicabili sulle stringe.

Table 4. string Operazioni di concatenamento di stringhe

Simbolo	Valore (hex)	Descrizione
OP_CAT	0x7e	Disabilitato (concatena i due elementi in cima)
OP_SUBSTR	0x7f	Disabilitato (ritorna una sottostringa)
OP_LEFT	0x80	Disabilitato (ritorna il substring di sinistra)
OP_RIGHT	0x81	Disabilitato (ritorna il substring di destra)
OP_SIZE	0x82	Calcola la lunghezza della stringa dell'elemento in cima e pusha il risultato

Aritmetica binaria e condizionali mostra l'aritmetica binaria e gli operatori logici booleani

Table 5. Aritmetica binaria e condizionali

Simbolo	Valore (hex)	Descrizione
OP_INVERT	0x83	Disabilitato (Capovolge i bit dell'elemento in cima)

Simbolo	Valore (hex)	Descrizione
OP_AND	0x84	Disabilitato (Booleano AND dei due elementi in cima)
OP_OR	0x85	Disabilitato (Booleano OR dei due elementi in cima)
OP_XOR	0x86	Disabilitato (Booleano XOR dei due elementi in cima)
OP_EQUAL	0x87	Metti TRUE (1) se i due elementi in cima sono esattamente identici, altrimenti metti FALSE (0)
OP_EQUALVERIFY	0x88	Come OP_EQUAL, ma esegue OP_VERIFY dopo essersi fermato (halt) se non TRUE
OP_RESERVED1	0x89	Halt - Transazione invalida se non trovata in una clause OP_IF inaspettata
OP_RESERVED2	0x8a	Halt - Transazione invalida se non trovata in una clause OP_IF non eseguita

Operatori numerici mostra gli operatori numerici (aritmetici).

Table 6. Operatori numerici

Simbolo	Valore (hex)	Descrizione
OP_1ADD	0x8b	Aggiunge 1 all'elemento in cima
OP_1SUB	0x8c	Sottrae 1 dall'elemento in cima
OP_2MUL	0x8d	Disabilitato (moltiplica l'elemento in cima per 2)
OP_2DIV	0x8e	Disabilitato (dividi l'elemento in cima per due)
OP_NEGATE	0x8f	Inverti il segno dell'elemento in cima
OP_ABS	0x90	Cambia il segno dell'elemento in cima in positivo
OP_NOT	0x91	Se l'elemento in cima è 0 o 1 Booleano, invertilo, altrimenti ritorna 0
OP_0NOTEQUAL	0x92	Se l'elemento in cima è 0, ritorna 0, altrimenti ritorna 1
OP_ADD	0x93	Prendi (pop) i due elementi in cima aggiungili e metti il risultato in cima (push)

Simbolo	Valore (hex)	Descrizione
OP_SUB	0x94	Prendi i due elementi in cima, sottrai il primo dal secondo, fai push del risultato
OP_MUL	0x95	Disabilitato (moltiplica i due elementi in cima allo stack)
OP_DIV	0x96	Disabilitato (dividi il secondo elemento per il primo)
OP_MOD	0x97	Disabilitato (resto della divisione tra il secondo elemento per il primo elemento)
OP_LSHIFT	0x98	Disabilitato (shifta a sinistra i bit del secondo elemento per i bit indicati dal primo elemento)
OP_RSHIFT	0x99	Disabilitato (shifta il secondo elemento a destra per i bit indicati nel primo elemento)
OP_BOOLAND	0x9a	Booleano AND sui due elementi in cima
OP_BOOLOR	0x9b	Booleano OR sui due elementi in cima
OP_NUMEQUAL	0x9c	Ritorna TRUE se i due elementi in cima sono numeri uguali
OP_NUMEQUALVERIFY	0x9d	Identico a NUMEQUAL, poi OP_VERIFY per fermare se non è TRUE
OP_NUMNOTEQUAL	0x9e	Ritorna TRUE se i due elementi in cima non sono numeri uguali
OP_LESSTHAN	0x9f	Ritorna TRUE se il secondo elemento è inferiore all'elemento in cima
OP_GREATERTHAN	0xa0	Ritorna TRUE se il secondo elemento è più grande dell'elemento in cima
OP_LESSTHANOREQUAL	0xa1	Ritorna TRUE se il secondo elemento è inferiore o uguale all'elemento in cima
OP_GREATERTHANOREQUAL	0xa2	Ritorna TRUE se il secondo elemento è maggiore o uguale all'elemento in cima
OP_MIN	0xa3	Ritorna il più piccolo dei due elementi in cima
OP_MAX	0xa4	Ritorna il più grande dei due elementi in cima

Simbolo	Valore (hex)	Descrizione
OP_WITHIN	0xa5	Ritorna TRUE se il terzo elemento è tra il secondo elemento (o uguale) e il primo elemento

Operazioni crittografiche e di hashing mostra gli operatori di funzione crittografica.

Table 7. Operazioni crittografiche e di hashing

Simbolo	Valore (hex)	Descrizione
OP_RIPEMD160	0xa6	Ritorna l'hash RIPEMD160 dell'elemento in cima
OP_SHA1	0xa7	Ritorna l'hash SHA1 dell'elemento in cima
OP_SHA256	0xa8	Ritorna l'hash SHA256 dell'elemento in cima
OP_HASH160	0xa9	Ritorna l'hash RIPEMD160(SHA256(x)) dell'elemento in cima
OP_HASH256	0xaa	Ritorna l'hash SHA256(SHA256(x)) dell'elemento in cima
OP_CODESEPARATOR	0xab	Segna l'inizio di un dato signature-checked (controllato da firma)
OP_CHECKSIG	0xac	Pop a public key and signature and validate the signature for the transaction's hashed data, return TRUE if matching
OP_CHECKSIGVERIFY	0xad	Uguale a CHECKSIG, inoltre fa si che OP_VERIFY si fermi (halt) se non TRUE
OP_CHECKMULTISIG	0xae	Esegui CHECKSIG per ogni coppia di firma e public key fornita. Tutte devono corrispondere. Un bug nell'implementazione fa il pop di un valore extra, usa il prefisso NO_OP come workaround.
OP_CHECKMULTISIGVERIFY	0xaf	Uguale a CHECKMULTISIG, inoltre fa si che OP_VERIFY si interrompa (halt) se non TRUE

Non-operatori mostra simboli nonoperator

Table 8. Non-operatori

Simbolo	Valore (hex)	Descrizione
OP_NOP1-OP_NOP10	0xb0-0xb9	Non fa niente, ignorato

OP code riservati per uso interno dal parser mostra i codici operatori riservati all'uso per lo script interno di parsing.

Table 9. OP code riservati per uso interno dal parser

Simbolo	Valore (hex)	Descrizione
OP_SMALLDATA	0xf9	Rappresenta un campo dati piccolo
OP_SMALLINTEGER	0xfa	Rappresenta un campo dati per un intero piccolo
OP_PUBKEYS	0xfb	Rappresenta i campi della public key
OP_PUBKEYHASH	0xfd	Rappresenta un campo per un hash di una chiave pubblica
OP_PUBKEY	0xfe	Rappresenta un campo per una chiave pubblica
OP_INVALIDOPCODE	0xff	Rappresenta un qualsiasi OP code non attualmente assegnato